kaspersky BRING ON THE FUTURE

Kaspersky Managed Detection and Response

Most security teams take an alert-driven approach to cybersecurity incidents, reacting only after an incident has already taken place. Meanwhile, new threats move in under the radar, leaving you with a false sense of security – literally. Businesses are increasingly recognizing the need to proactively hunt out threats lying undiscovered but still active within their corporate infrastructures.

Service benefits:

- The reassurance of knowing that you are continuously protected against even the most innovative threats
- Reduced overall security costs without the need to employ a range of in-house security specialists
- Focusing expensive in-house resources on those critical tasks that really require their involvement
- All the major advantages from having your own security operations center without having to actually establish one

Kaspersky Managed Detection and Response (MDR) delivers advanced, round-the-clock protection from the growing volume of threats circumventing automated security barriers, providing relief to organizations struggling to find specialized staff or with limited in-house resources.

Its superior detection and response capabilities are supported by one of the most successful and experienced threat hunting teams in the industry. Unlike similar offerings on the market, Kaspersky MDR leverages patented machine-learning models, unique ongoing threat intelligence and a proven track record of effective targeted attack research. It automatically strengthens your corporate resilience to cyberthreats while optimizing your existing resources and future IT security investments.

Service highlights

- Fast, scalable turnkey deployment enables an instantly matured IT security function without the need to invest in additional staff or expertise
- Superior protection against even the most complex and innovative non-malware threats prevents business disruption and minimizes overall incident impact
- Completely managed or guided incident response provides a swift reaction while keeping all response actions within your full control
- Real-time visibility across your assets and their protection status delivers ongoing situational awareness through various communication channels

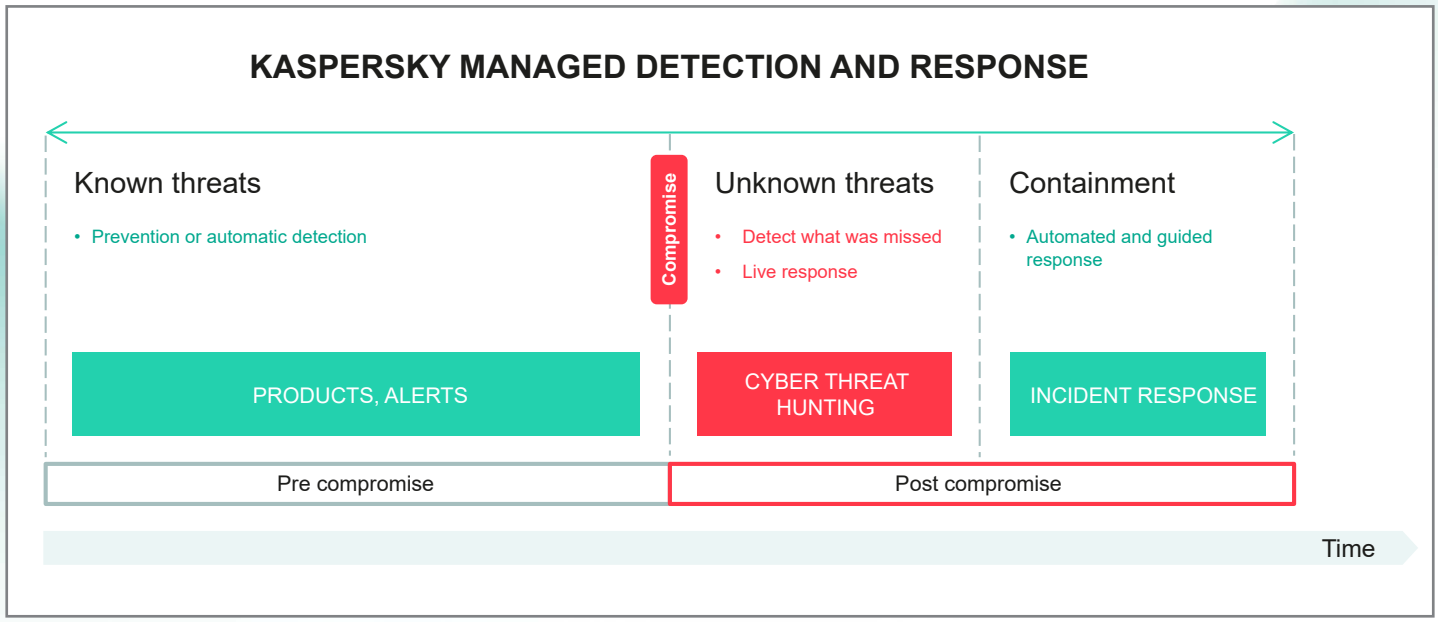

Figure 1. Kaspersky Managed Detection and Response

Supported products:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Security for Windows Server
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

How it works

Kaspersky MDR validates product alerts to ensure the effectiveness of automatic prevention and proactively analyzes system activity metadata for any signs of an active or impending attack. This metadata is collected via Kaspersky Security Network, and is automatically correlated in real-time with Kaspersky's unequalled threat intelligence to identify the tactics, techniques and procedures used by attackers. Proprietary Indicators of Attack enable the detection of stealthy non-malware threats mimicking legitimate activity. The service adapts to your infrastructure during the first 2-4 weeks, to ensure zero false positive rates, confirming with you what is legitimate and what is not.

Kaspersky MDR features two tiers to suit the needs of organizations of every size and industries with varying IT security maturity levels (Figure 2). **Kaspersky MDR Optimum** instantly raises your IT security capability without the need to invest in additional staff or expertise and provides resilience to evasive attacks through its fast, turnkey deployment. **Kaspersky MDR Expert** includes all the features of Optimum and provides extended functionality and flexibility for mature IT security teams, enabling them to offload incident triage and investigation processes to Kaspersky and focus their limited in-house IT security resources on reacting to the critical outcomes delivered.

Figure 2. Kaspersky MDR tiers

Automated threat hunting included in MDR Optimum uses automatic detections based on proprietary Indicators of Attack (IoA). These detections are made on real-time and historical telemetry, and are used by our SOC analysts to further identify, validate and investigate threats. Kaspersky SOC uses 700+ proprietary Indicators of Attack covering 100% of all known adversarial Tactics, Techniques and Procedures (TTPs).

At the same time, **managed threat hunting** in MDR Expert relies on the painstaking, hands-on efforts of our experienced threat hunters and is tailored to your specific infrastructure. Our threat hunting team proactively hunts out previously unknown TTPs that do not result in automatic detection. If such TTPs are identified, the team develops new or adjusts existing Indicators of Attack for future use in both MDR tiers.

A set of complementary optional elements tailor the functionality of the service to your specific requirements, providing enhanced flexibility when needed.

Countering targeted attacks requires extensive experience as well as constant learning. As the first vendor to establish, almost a decade ago, a dedicated center for investigating complex threats, Kaspersky has detected more sophisticated targeted attacks than any other security solution provider. Leveraging this unique expertise, Kaspersky Managed Detection and Response maximizes the value of your Kaspersky security solutions by delivering a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. This is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Proven.
Transparent.
Independent.